PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/08, H04Q 7/22	A1	(11) International Publication Number: WO 99/01848 (43) International Publication Date: 14 January 1999 (14.01.99)

(21) International Application Number: PCT/FI98/00522

(22) International Filing Date: 16 June 1998 (16.06.98)

(30) Priority Data:
972840 2 July 1997 (02.07.97) FI

(71) Applicant *(for all designated States except US)*: SONERA OY [FI/FI]; Sturenkatu 16, FIN–00510 Helsinki (FI).

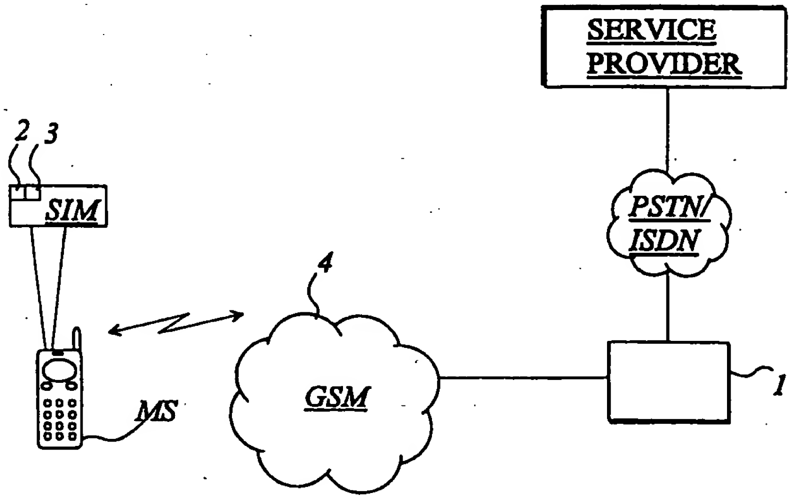
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: VATANEN, Harri [FI/FI]; Sonera Oy, Sturenkatu 16, FIN–00510 Helsinki (FI).

(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN–00101 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: PROCEDURE FOR THE CONTROL OF APPLICATIONS STORED IN A SUBSCRIBER IDENTITY MODULE



(57) Abstract

The invention relates to a procedure for the control of applications stored in a subscriber identity module in a data communication system comprising a data communication network (4), a terminal device (MS) connected to the data communication network, a subscriber identity module (SIM) connected to the terminal device and containing a stored application that makes use of the data communication network and is used by means of the terminal device, and an application control server (1) connected to the data communication network. In an embodiment of the invention, a key list comprising one or more application–specific keys is stored in the subscriber identity module (SIM). A corresponding list is also stored in the application control server, which takes care of the control of applications stored in subscriber identity modules. The application stored in the subscriber identity module is activated and/or closed by using the key list.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	**Albania**
AM	**Armenia**
AT	**Austria**
AU	**Australia**
AZ	**Azerbaijan**
BA	**Bosnia and Herzegovina**
BB	**Barbados**
BE	**Belgium**
BF	**Burkina Faso**
BG	**Bulgaria**
BJ	**Benin**
BR	**Brazil**
BY	**Belarus**
CA	**Canada**
CF	**Central African Republic**
CG	**Congo**
CH	**Switzerland**
CI	**Côte d'Ivoire**
CM	**Cameroon**
CN	**China**
CU	**Cuba**
CZ	**Czech Republic**
DE	**Germany**
DK	**Denmark**
EE	**Estonia**
ES	**Spain**
FI	**Finland**
FR	**France**
GA	**Gabon**
GB	**United Kingdom**
GE	**Georgia**
GH	**Ghana**
GN	**Guinea**
GR	**Greece**
HU	**Hungary**
IE	**Ireland**
IL	**Israel**
IS	**Iceland**
IT	**Italy**
JP	**Japan**
KE	**Kenya**
KG	**Kyrgyzstan**
KP	**Democratic People's Republic of Korea**
KR	**Republic of Korea**
KZ	**Kazakstan**
LC	**Saint Lucia**
LI	**Liechtenstein**
LK	**Sri Lanka**
LR	**Liberia**
LS	**Lesotho**
LT	**Lithuania**
LU	**Luxembourg**
LV	**Latvia**
MC	**Monaco**
MD	**Republic of Moldova**
MG	**Madagascar**
MK	**The former Yugoslav Republic of Macedonia**
ML	**Mali**
MN	**Mongolia**
MR	**Mauritania**
MW	**Malawi**
MX	**Mexico**
NE	**Niger**
NL	**Netherlands**
NO	**Norway**
NZ	**New Zealand**
PL	**Poland**
PT	**Portugal**
RO	**Romania**
RU	**Russian Federation**
SD	**Sudan**
SE	**Sweden**
SG	**Singapore**
SI	**Slovenia**
SK	**Slovakia**
SN	**Senegal**
SZ	**Swaziland**
TD	**Chad**
TG	**Togo**
TJ	**Tajikistan**
TM	**Turkmenistan**
TR	**Turkey**
TT	**Trinidad and Tobago**
UA	**Ukraine**
UG	**Uganda**
US	**United States of America**
UZ	**Uzbekistan**
VN	**Viet Nam**
YU	**Yugoslavia**
ZW	**Zimbabwe**

PROCEDURE FOR THE CONTROL OF APPLICATIONS STORED IN A SUBSCRIBER IDENTITY MODULE

The present invention relates to a procedure as defined in the preamble of claim 1 for verifying the rights relating to the control of keys to applications stored in a subscriber identity module and to the use of such applications.

With the development of mobile communication networks, especially GSM networks (GSM, Global System for Mobile Communications), the services offered through them develop as well. Especially in applications making use of mobile communication networks and requiring a high level of data security, e.g. in payments for services, ordering, order confirmations, payment orders, bank services, etc., problems are encountered regarding safe application-specific control of keys and billing of license fees for operator-independent services. The problem is accentuated by the fact that subscriber identity modules used in GSM terminals are manufactured by several enterprises and that there are many companies offering applications and several operators delivering subscriber identity modules to customers. In addition, the applications used to provide services in the GSM network are often produced by outside software suppliers or equivalent, which means that the licenses for the applications belong to the software suppliers.

If a license fee is to be charged for the use of an application, it is necessary to carefully follow the use of the application and define the limits within which the application may be used. For this purpose no solution has been presented before, at least no solution that allows centralised control of the subscriber identity modules and the passwords relating to the applications stored in them.

The object of the present invention is to eliminate the drawbacks described above.

A specific object of the present invention is to produce a new type of procedure which is applicable for the control of keys to applications making use of the subscriber identity module and for the control of license agreements concerning the use of such applications and which can be easily implemented in a centralised form independent of different suppliers.

A further object of the present invention is to produce a procedure with a high level of data security that allows flexible and reliable safeguarding of the interests of operator, module manufacturer, application developers and users of applications.

As for the features characteristic of the invention, reference is made to the claims.

In conjunction with the present procedure for the control of applications stored in a subscriber identity module, the data communication system preferably comprises a data communication network and a terminal device connected to the data communication network. Preferably the data communication network is a GSM network and the terminal device is a GSM telephone. The GSM telephone is preferably provided with a subscriber identity module containing an application stored in it, which utilises the data communication network and is used via the terminal device for bank or other services available. The data communication system also comprises an application control server (1) connected to the data communication network. The application control server is preferably a computer or equivalent which is provided with means for setting up a connection to the data communication network and with software for implementing the required applications. The software is preferably managed by service providers or especially by data communication suppliers providing management services.

According to the invention, a key list comprising one or more application-specific keys is stored in the subscriber identity module. The key list is preferably linked or connected with the subscriber identity module by using a unique identifier corresponding to the module. A corresponding list is also stored in the application control server, and the application stored in the subscriber identity module is activated and/or closed using the key list.

Thus, in the procedure of the invention, stored on a smart card (SIM card) in the mobile station is a list of keys comprising the keys K(1), K(2), ..., K(n) and KA(1) and KA(2) needed for activating or closing different applications on the card. The SIM card or subscriber identity module preferably also contains modules for activating and closing the application. In conjunction with manufacture, the SIM card has been initialised with a security module in a known manner. The activating/closing module is used to ensure that the application, such as electronic signature utilising the smart card, can be activated/closed by the key control system if necessary. Thus, the procedure of the invention implements application-specific key control in addition to the previously known SIM card key control system.

The application-specific key control system knows the keys needed in an application or applications, and these keys need not be known to the mobile communication operator's key control system. The application-specific key control system of the invention can be separated from the operators' key control systems, thus making it possible to provide a service independent of data communication network and operator. The key control system responsible for the applications need not know the teleoperator's keys, which are used for user identification in basic mobile communication services in a manner known in itself. Key control for applications is implemented in a protected database, from which application-specific services utilising the SIM card and requiring a high level of data security can be activated and closed.

As compared with prior art, the invention has the advantage that the procedure allows local identification of the user of services requiring a high level of data security by all service providers in the networks of different operators as well as a centralised implementation of key control.

Moreover, the procedure of the invention allows control and billing of user-specific payments and licenses for different applications.

In an embodiment of the invention, the validity of the user's right of access to the application stored in the subscriber identity module is verified periodically. If it is established that the access right has expired, then, using an appropriate key, the application in the subscriber identity module can be closed.

In conjunction with the activation of the application stored in the subscriber identity module, the subscriber identity module is sent a message concerning the opening of the application, said message containing the application key k(n) to be used in the application. In the application control server, the application key is attached to the unique identifier corresponding to the subscriber identity module. Based on the key list, the right of access to the application is preferably verified in the application control server and, if a valid access right exists, the special data needed in the application, e.g. service description and application-specific user interface codes, are sent.

In an embodiment of the present invention, all messages between the application control server and the terminal device are encrypted regardless of the content of the message.

In the following, the invention will be described by the aid of embodiment examples by referring to the attached drawing, in which

Fig. 1 presents a preferred data communication system in which the procedure of the invention can be used; and

Fig. 2 presents a block diagram of a preferred embodiment of the procedure of the invention.

Fig. 1 presents an example of a data communication system in which the procedure of the invention can be implemented. The data communication system shown in Fig. 1 comprises a GSM telephone network 4. Connected to the GSM network is a mobile station MS compatible with the network and provided with a subscriber identity module SIM. In conjunction with manufacture, the subscriber identity module SIM has been initialised using a security module in a manner known in itself; reference is made to patent specification WO 90/11849. Moreover, the subscriber identity module comprises an activating and closing module 2, 3, which are used for the activation and closing of the application.

The service provider's application control server 1 is connected to the GSM network and to the service provider's equipment e.g. via a telephone network PSTN/ISDN. The connection between the application control server 1 and the GSM telephone MS is set up in accordance with the normal GSM practice either as a voice, data or short message connection. Let it be further stated that the telephone network 4 may be any other data communication network, such as a CDMA network, PCN network, UMTS network or equivalent, and that, correspondingly, the terminal device may be any other terminal device compatible with the data communication network to which a subscriber identity module or an equivalent device can be connected.

Fig. 2 presents a block diagram illustrating the various stages of control of an application in the subscriber identity module, carried out by the application control server. The example used here is a bank application in which a bank gives its customer the right to use its bank services using a GSM telephone MS and an application stored in a subscriber identity module SIM connected to it.

The customer is in possession of an identifier (UID) corresponding to the SIM card. The key k(n) corresponding to the identifier (UID) and the application (n) as well as the keys KA1 and KA2 have been stored in an application-specific key control system in the application control server 1. The customer makes an agreement with the bank about the use of a mobile station based bank service, whereupon the bank sends the UID corresponding to the customer's SIM card to an application-specific card control system. After this, the application-specific card control system sends an opening message to the SIM card corresponding to the UID. The opening message contains the customer's user key k(n) which is needed for the bank service and which is to be used later to activate the application stored on the card, and a possible registering message. Using the key k(n) sent by the card control system, the customer can set the mobile station to bank mode and send and acknowledgement of the registering message to the card control system. The key k(n) can also be sent in an encrypted form, which is decrypted by a decryption programme on the SIM card. The customer now has a licensed key that gives him/her the right to use the bank service concerned. The key is useless to outsiders because it is card-specific and will only activate an application stored on the particular card.

c ②

In conjunction with the activation of the card, the customer may be billed for the license fees if the customer acknowledges the registration. The application-specific card control system sends to the bank the necessary identifiers, including the identifier KA(1) needed for the activation of a bank service. In the bank, the customer and application specific identifier sent by the card control system is associated with the respective bank service. Using the application-specific activation code KA(1), the bank can load the service menus and forms needed in the bank service as well as the identifiers needed in the use of the service onto the customer's card, whereupon the bank service is available to the customer. The bank-specific service menus and service forms are transmitted to the mobile station by the "dynamic menu load" method or to the SIM card by the OTA (Over The Air) method in a manner known in itself. If the code KA(1) is correct, the activating/closing module on the card will accept the loading and the card will be activated for the bank service.

Finally, the process described above will be presented in greater detail by referring to the block diagram in Fig. 2. At a bank, the customer makes an agreement about utilising a mobile station MS and linking it to a bank service, block 21. At the same time, the unique identifier (UID) of the customer's subscriber identity module is linked to the service as described above. In the agreement, the customer accepts the license conditions required for the use of the application. Via the application control server 1, the bank sends the unique identifier (UID) of the subscriber identity module for the activation of the application in the subscriber identity module to the application-specific subscriber identity module control system, block 22. The subscriber identity module control system initialises the subscriber identity module SIM by sending a registering confirmation to the customer's mobile station, block 23. At the same time, the customer receives a key k(n) that the customer can use to switch his/her mobile station and the associated subscriber identity module into bank mode and subsequently to open the service.

In block 24, the customer enters the key k(n) into the mobile station and accepts the registration by acknowledging the registering message sent by the subscriber identity module control system. After this, the subscriber identity module control system sends the keys needed for the use of the application to the bank so that the application-specific menus and customer identifiers can be loaded into the customer's mobile station and subscriber identity module, block 25. The customer's mobile station has now been opened and activated and is ready for use in the bank service, block 26. If the customer misuses the system or otherwise fails to observe the terms of agreement, then the subscriber identity module control system can close the application in the subscriber identity module. The application is closed using a closing message containing a closing key.

If the customer fails to make the payments to be subsequently charged for the use of the application, e.g. the annual license fee to be paid for the service, use of the application can be prevented by sending the subscriber identity module SIM a closing message from the key control system. The encrypted closing message contains a closing key by which the application in the subscriber identity module will recognise that the sender of the message has the right to close the application stored on the card. Similarly, if the mobile station together with the subscriber identity module is lost, the card or application can be closed. The application can be opened and activated again in a corresponding manner from the application-specific key control system.

The invention is not restricted to the examples of its embodiments described above, but many variations are possible within the scope of the inventive idea defined by the claims.

CLAIMS

1. Procedure for the control of applications stored in a subscriber identity module in a data communication system comprising a data communication network (4), a terminal device (MS) connected to the data communication network, a subscriber identity module (SIM) connected to the terminal device and containing a stored application that makes use of the data communication network and is used by means of the terminal device, and an application control server (1) connected to the data communication network, characterised in that

a key list comprising one or more application-specific keys is stored in the subscriber identity module (SIM);

a key list corresponding to the key list stored in the subscriber identity module is stored in the application control server; and

the application stored in the subscriber identity module is activated and/or closed using the key list.

2. Procedure as defined in claim 1, characterised in that a module (2, 3) for activating and/or closing the application is stored in the subscriber identity module (SIM).

3. Procedure as defined in claim 1 or 2, characterised in that a check is carried out periodically to determine whether a valid right of access to the application stored in the subscriber identity module exists.

4. Procedure as defined in any one of the preceding claims 1 - 3, characterised in that, in the application control server, the key list is linked to the subscriber identity module by using a unique identifier corresponding to it.

5. Procedure as defined in any one of the preceding claims 1 - 4, characterised in that, by means of the application control server (1),

a message concerning the opening of the application and containing an application key k(n) to be used in the application is sent to the subscriber identity module; and

the application key is attached to the unique identifier corresponding to the subscriber identity module.

6. Procedure as defined in any one of the preceding claims 1 - 5, characterised in that, via the application control server (1),

the right of access to the application is verified on the basis of the key list; and

the special data needed in the application are sent if a valid access right exists.

7. Procedure as defined in any one of the preceding claims 1 - 6, characterised in that the messages between the application control server (1) and the terminal device (MS) are encrypted.

8. Procedure as defined in any one of the preceding claims 1 - 7, characterised in that a telecommunication connection is set up between the terminal device (MS) and the subscriber identity module (SIM) connected to it on the one hand and the application control server (1) on the other hand via a telephone network, such as a mobile communication network.

9. Procedure as defined in any one of the preceding claims 1 - 9, characterised in that the data communication network (4) is a GSM network and the terminal device (MS) is a GSM telephone.

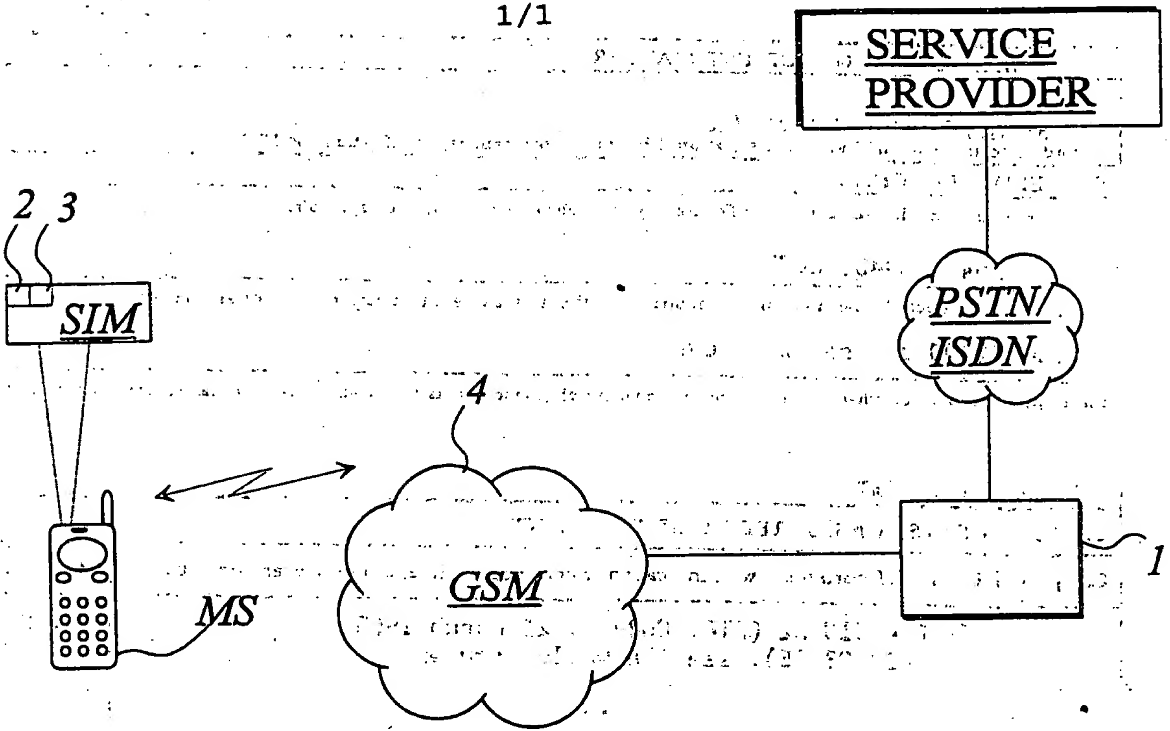

SERVICE PROVIDER
2
3
SIM
PSTN/ ISDN
4
GSM
MS
1

Fig 1

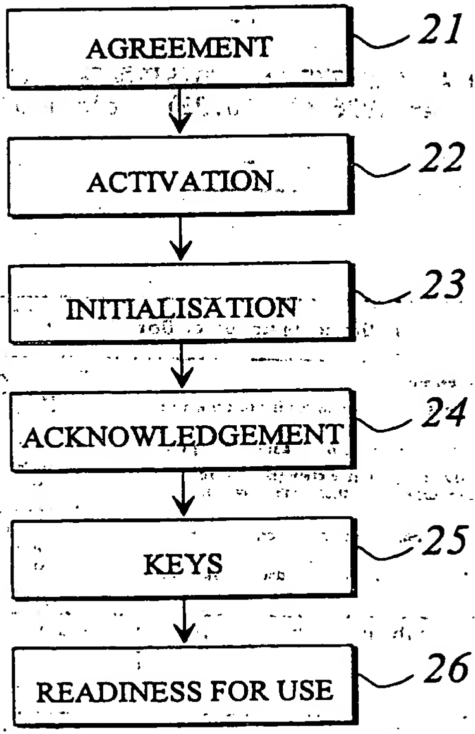

AGREEMENT
21
ACTIVATION
22
INITIALISATION
23
ACKNOWLEDGEMENT
24
KEYS
25
READINESS FOR USE
26

Fig 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00522

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G07F 7/08, H04Q 7/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04Q, G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPI, PAT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0644513 A2 (AT&T CORP.), 22 March 1995 (22.03.95), see the whole document --	1-9
Y	EP 0748135 A2 (CELLTRACE COMMUNICATIONS LIMITED), 11 December 1996 (11.12.96), column 2, line 1 - line 26; column 3, line 2 - line 7; column 4, line 6 - line 11, figure 1, column 6, line 49 - line 56 --	1-9
Y	WO 9632700 A1 (AU-SYSTEM, JONSTRÖMER, ULF), 17 October 1996 (17.10.96), claim 8 -- -----	1-9

□ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" erlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 8 December 1998	Date of mailing of he international search report 11 -12- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Peter Hedman Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/FI 98/00522

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0644513 A2	22/03/95	CA 2131510 A	18/03/95
		JP 7152837 A	16/06/95
		NO 943457 A	20/03/95
		US 5544246 A	06/08/96
EP 0748135 A2	11/12/96	AU 691812 B	28/05/98
		AU 6934694 A	03/01/95
		BR 9406850 A	27/05/97
		CA 2165201 A	22/12/94
		CN 1127579 A	24/07/96
		CZ 9503284 A	12/06/96
		EP 0704140 A	03/04/96
		EP 0865217 A	16/09/98
		FI 956022 A	14/02/96
		HU 73898 A	28/10/96
		HU 9503602 D	00/00/00
		JP 8511387 T	26/11/96
		NO 955079 A	18/01/96
		PL 312223 A	01/04/96
		WO 9430023 A	22/12/94
		ZA 9404242 A	15/12/95
WO 9632700 A1	17/10/96	AU 3943795 A	06/06/96
		EP 0784715 A	23/07/97
		JP 10508904 T	02/09/98
		NO 974626 A	13/10/97
		SE 506506 C	22/12/97
		SE 9501347 A	12/10/96